Department of Homeland Security Daily Open Source Infrastructure Report for 5 May 2008

Current Nationwide Threat Level is
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
For info click here
http://www.dhs.gov/

- According to CNN, the U.S. Air Force grounded all T-38C training jets Thursday after the second fatal crash involving the aircraft in eight days. Two pilots died when their high-altitude supersonic plane went down during a routine training mission. (See item **8**)
- WRAL 5 Raleigh reports two men were arrested Wednesday in North Carolina after their homemade bomb exploded prematurely, injuring both. The pair had made several bombs at their home, and one of them tried to throw one out the window of a minivan as they drove past two schools. (See item **22**)

DHS Daily Open Source Infrastructure Report Fast Jump

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − [http://www.esisac.com]

1. *May 2, Hess Corporation* – (International) **ExxonMobil reaches strike agreement.** Four out of five strikers' demands have been met by ExxonMobil that has led to the immediate resumption of oil production in Nigeria. "We have reached agreement, production resumes immediately," said the chairman of the Pengassan union's Mobil Producing Nigeria branch. The eight-day strike led to the closure of many U.S. oil major's production in the country and led to the petroleum company failing to meet its contractual obligations on deliveries. Attacks by Niger Delta rebels have also affected ExxonMobil's production and have contributed to the rising price of oil.
Source: http://www.hessenergy.com/common/NewsItem.aspx?ArticleId=18578250

2. *May 2, CBS News and Associated Press* – (Midwest) **Powerful Midwest storms leave deadly trail.** Tornadoes and severe storms ripped through Arkansas, Missouri, Oklahoma, and Texas late Thursday and early Friday. In Kansas City, Missouri, about 40,000 lost power at the peak of the storm Thursday. In Canton, Texas, local officials said an apparent tornado Friday ripped down power lines.
   Source: http://www.cbsnews.com/stories/2008/05/02/national/main4064959.shtml

3. *May 2, Associated Press* – (Kansas) **Governor's veto of coal bill stands.** Supporters of two coal-fired power plants have failed to override the governor's veto of a bill allowing the plants in southwest Kansas. The vote Thursday night in the House was 80-45; supporters were four votes short. But some of them are promising to keep trying to enact a law to make sure Sunflower Electric Power Corp. can build the plants outside Holcomb, in Finney County. "It's not over until the Legislature adjourns, and they're still in session," said the utility's chief executive officer. The Kansas Department of Health and Environment secretary denied an air-quality permit for Sunflower's project in October because of the plants' potential carbon dioxide emissions.
   Source: http://www.thekansan.com/news/x1838798194

4. *May 2, Pittsburgh Tribune-Review* – (Ohio) **Power plant made in Versailles starts up.** An Ashta Chemicals Inc. plant in Ohio has begun to generate some of the electricity it uses with HydroGen Corp.'s first fuel cell power installation, made at its factory in Versailles, Ohio. HydroGen said this week that Ashta started up its 400-kilowatt plant as a demonstration project partly funded with a $1.25 million grant from the state of Ohio. HydroGen is commercializing a phosphoric acid fuel cell technology that Westinghouse developed in the 1980s, targeting chemical companies as well as coke-making, gas production, and other industries that produce hydrogen as a waste or byproduct. The installation at Ashta, now undergoing testing, will be a prototype for other plants, the company said.
   Source: http://www.pittsburghlive.com/x/pittsburghtrib/business/s_565406.html

5. *May 2, Philadelphia Inquirer* – (Pennsylvania) **Exelon considering new power plant for region.** Exelon Corp. said Thursday that it hoped to build a new power plant in the Philadelphia area to serve more than half a million households. Exelon said its 600-megawatt plant, to be completed no sooner than 2012, would cost about $700 million. It will burn natural gas.
   Source:
   http://www.philly.com/inquirer/business/20080502_Exelon_considering_new_power_plant_for_region.html

[Return to top]

Chemical Industry Sector

6. *May 2, KRGV 5 Weslaco* – (Texas) **Helena cleanup meeting.** The Environmental Protection Agency held what was supposed to be a question and answer session for residents living near the old Helena Chemical Plant site in Mission, Texas. The purpose

of the meeting was to inform the public that the clean up was complete, and the site is ready for commercial or industrial use. The residents did not agree, many gathering to express their concerns over the site's history, and possible health impacts. Officials with the Texas Health Department say, the chemical levels in the soil in the area pose no danger, and there is no way to link the diseases in the area to the chemicals.
Source: http://www.newschannel5.tv/2008/5/2/990644/Helena-Cleanup-Meeting

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

Nothing to Report

[Return to top]

Defense Industrial Base Sector

7. *May 2, Strategy Page* – (National) **U.S. Army back in orbit.** The U.S. Army is back in the satellite launching business, 52 years after it lost its long range ballistic missiles and satellite launchers to the Air Force. The Army is developing a nano-satellite for deploying quick satellite communications capability in parts of the world that are poorly served by military satellites. The new system would use a swarm of five pound satellites, launched using retired and refurbished Minuteman rockets or other commercial rockets.
Source: http://www.strategypage.com/htmw/htspace/articles/20080502.aspx

8. *May 1, Associated Press* – (National) **Air Force grounds T-38s after fatal crashes.** The Air Force grounded all T-38C training jets Thursday after the second fatal crash involving the aircraft in eight days, the military said. Two pilots died when their high-altitude supersonic plane went down during a routine training mission, according to a statement from Sheppard Air Force Base in Texas. The two-seat plane was assigned to the 80th Flying Training Wing, a multinational organization that produces future combat pilots for NATO. The crash follows the deaths of two pilots whose training jet crashed April 23 at Columbus Air Force Base in Mississippi. "At this point, we have no indication that there was any tie between the two," said the chief of media relations for Air Education Training Command at Randolph Air Force Base near San Antonio. The Air Force suspended all T-38 flights pending the investigations into what caused the two planes to go down.
Source: http://www.cnn.com/2008/US/05/01/jet.crash.ap/index.html

9. *May 2008, National Defense* – (National) **'IED Defeat Task Force' also in the private sector.** When the U.S. Defense Department launched its campaign against roadside bombs, it reached out to defense contractors and academia for technologies to counter improvised explosive devices (IEDs). It created the Joint IED Defeat Organization (JIEDDO) to evaluate, test, and acquire technologies. Last month, Raytheon unveiled its "Raytheon IED-Defeat Task Force," with a website to recruit industry and academic partners to help defeat improvised explosive devices. Raytheon "supports the JIEDDO

effort and works within the JIEDDO process to develop and field IED solutions to our war fighters," says the director of the Raytheon IED Defeat Task Force.
Source:
http://www.nationaldefensemagazine.org/issues/2008/May/Washington.htm#Joint

10. *May 2008, National Defense* – (National) **Wanted: One unmanned aerial vehicle; must be able to take off from ships.** The U.S. Coast Guard is in the market for a new vertical unmanned aerial vehicle (UAV) to fly off the deck of its new national security cutters. A UAV is needed in the Integrated Deepwater System to provide long-range over the horizon intelligence, reconnaissance, and surveillance. The Coast Guard will take a look at any UAV that meets its requirements, but it has to be fully tested and ready to go into production before the service will consider it, said the service's assistant commissioner for acquisition. One possible solution is the Navy's MQ-8B Fire Scout, manufactured by Northrop Grumman, he said. The problem is that the rotary-wing UAV does not have an integrated radar in its sensor suite. The Navy is looking at adding funds in the 2009 and 2010 budget requests to do so. Northrop was spending some of its own funds to add radar capabilities onto the unmanned helicopter, he said.
Source:
http://www.nationaldefensemagazine.org/issues/2008/May/SecurityBeat.htm#Wanted

[Return to top]

Banking and Finance Sector

11. *May 2, Associated Press* – (National) **Government cracks down on credit card industry practices.** The Federal Reserve and two government agencies are proposing rules that would stop credit card companies from unfairly raising interest rates and make sure they give people enough time to pay their bills. The proposed new rules would prohibit placing unfair time constraints on payments; a payment could not be deemed late unless the borrower is given a reasonable period of time, such as 21 days, to pay; unfairly allocating payments among balances with different interest rates; unfairly raising annual percentage rates on outstanding balances; placing too-high fees for exceeding the credit limit solely because of a hold placed on the account; unfairly computing balances; unfairly adding security deposits and fees for issuing credit or making credit available; and making deceptive offers of credit. The banking industry is expected to fight the new rules.
Source:
http://news.yahoo.com/s/ap/20080502/ap_on_bi_ge/credit_card_rules;_ylt=AsonEoweVBodas20pvGD0eOs0NUE

12. *May 1, Computerworld* – (California) **California court posting SSNs and other personal data, privacy advocates charge.** Privacy advocates claim that Social Security numbers, medical histories, tax records, bank account data and other sensitive personal data are freely available online via the Web site of the Superior Court in California's Riverside County. Searches done on the court's Web site by Computerworld, using case numbers provided by a Virginia-based privacy advocate, turned up various documents related to civil cases that contained sensitive information. Included were complete tax

filings, medical reports pertaining to cases handled by the court, and images of checks complete with signatures as well as account and bank-routing numbers. But the court's IT director defended the practices, saying that documents are being posted on the Web site in accordance with California laws and that finding data such as Social Security numbers is akin to "finding a needle in a haystack." Altogether, the Web site potentially holds "thousands and thousands" of documents with personally identifiable information, contended the owner of a Web site called the Virginia Watchdog. It was not possible to verify that claim, nor was it immediately clear how easily accessible the personal data is.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9081858&taxonomyId=17&intsrc=kc_top

[Return to top]

Transportation Sector

13. *May 2, Sify News* – (International) **Hijack threat delays Mumbai-New York flight.** A Delta Airlines Mumbai-New York flight was delayed briefly late Thursday after the U.S. consulate in Mumbai, India, received a hijack threat that turned out to be false, an airport official said. The consulate informed the station manager of Delta Airlines that they have received the threat for flight DL-17, the official said. When contacted, the consulate spokesperson and station manager of Delta Airlines denied the incident completely. However, a police official confirmed the incident and told IANS, "We got a call from the airport authorities regarding a hijack threat and a suspect on board. We immediately deployed our team there." The airport police said it was almost like a non-incident. "But there was stringent security as a precautionary measure," he said.
Source**:** http://sify.com/news/fullstory.php?id=14663374

14. *May 2, Associated Press* – (National) **Western ports return to normal after workers' war protest.** West Coast cargo traffic came to a halt Thursday as port workers ditched the day shift, saying they wanted to commemorate May Day and call on the U.S. to end the war in Iraq. Thousands of dockworkers at 29 ports in California, Oregon and Washington were no-shows for the morning shift, leaving ships and trucks idle at ports from Long Beach to Seattle, said a Pacific Maritime Association spokesman. The West Coast ports are the nation's principal gateway for cargo container traffic from the Far East, with the adjacent ports of Los Angeles and Long Beach handling about 40 percent of the nation's cargo.
Source:
http://ap.google.com/article/ALeqM5hu9p3N4nCLP46UuEMxAIR_n2mgtgD90D8QRO0

15. *May 2, Boston Herald* – (Massachusetts; National) **Logan to get program to ease foreign-traveler entry.** U.S. Customs and Border Protection will add Logan International Airport in Boston, Massachusetts, to a new program designed to make travelers' entrances into the United States a more streamlined and user-friendly process. Logan and 17 other airports were selected for the Model Ports Initiative based on the number of foreign visitors they handle annually. The Model Ports Initiative is part of a

three-prong plan unveiled in 2006 to improve border security with the use of new technology, while streamlining security processes and easing travel for legitimate visitors. Elements include a video in Spanish, French, German and English that helps travelers through the customs and immigration process, an increased number of video monitors, a "Welcome to the U.S." brochure and bilingual directional signs.
Source: http://www.bostonherald.com/business/general/view.bg?articleid=1091126

16. *May 1, Cleveland Leader* – (National) **TSA now permits airlines to store birth dates, bringing relief to some.** The Transportation Security Administration (TSA) is now permitting airlines to store passengers' birth dates. The people who will benefit most from this change are those who have similar names to one on a terrorist watchlist, and who are routinely confused for being a terrorist themselves. The TSA says that by storing birth dates, the airlines will be able to more quickly verify that you are not the same person on the list. Right now, TSA keeps two lists: a strict "no fly" list, and another list that flags passengers for special attention at airport check-in and security. Those with names that match those on watchlists are currently barred from checking in for their flights online. Instead, they must present themselves to an agent at their airport.
Source: http://www.clevelandleader.com/node/5455

[Return to top]

Postal and Shipping Sector

Nothing to Report

[Return to top]

Agriculture and Food Sector

Nothing to Report

[Return to top]

Water Sector

17. *May 2, Associated Press* – (Arizona) **Contamination at Scottsdale water plant was operator error.** A malfunction at a Scottsdale, Arizona, plant that resulted in a three-day water ban affecting nearly 5,000 customers is being blamed on operator error. That is the conclusion of an investigation conducted for companies that were the source of the trichloroethylene contamination decades ago. The companies are paying for cleanup of the contaminated groundwater, including the treatment facility. The malfunction occurred January 15 at a plant owned and operated by the Arizona American Water Company that treats groundwater contaminated with TCE, an industrial solvent and a suspected cancer-causing chemical. A separate investigation done for Arizona American concluded that the plant's systems and components were not designed or operated in an optimal manner.

Source: http://www.abc15.com/news/local/story.aspx?content_id=ea963849-089d-4eaa-a045-a8884cfdfa1d

18. *May 1, Dayton Daily News* – (Ohio) **Contaminated water plume outlined.** In Ohio, environmental investigators think they have determined the general outline of a contaminated ground water plume in the vicinity of the Behr Dayton Thermal Plant. But the U.S. Environmental Protection Agency (EPA) and the plant's former owner, Chrysler, appear far apart on how to engineer a final cleanup. Negotiations between the EPA and the auto maker, which have broken down, also included talks with Behr representatives that dwelled on how to undertake a study to determine the nature and extent of contamination and the feasibility of cleanup options. Two other private businesses might share responsibility for the cleanup. A potential problem spot in the cleanup could be a large mass of contaminated soil beneath a factory complex owned by Behr GmbH & Co. The groundwater is contaminated with trichloroethylene, likely the result of an extensive industrial leak within the past 30 years, said the EPA on-scene coordinator. Soil gas from the groundwater has entered homes in the area of the plant, creating an indoor air health hazard at 251 addresses, the latest count suggests. The coordinator said he believes testing has revealed the approximate outline of the contaminated groundwater since the strength of the pollution diminishes along its borders.
Source: http://www.daytondailynews.com/n/content/oh/story/news/local/2008/05/01/ddn050108behr.html

[Return to top]

Public Health and Healthcare Sector

19. *May 2, VietNamNet Bridge* – (International) **Bird flu breaks out in one more southern province.** Bird flu has been discovered in the southern Vietnamese province of Vinh Long, killing nearly 400 chickens of a farmer family in Xuan Hiep commune, the local veterinary agency reported. Chickens there began dying on a massive scale on April 26. On April 28, the veterinary agency announced its test results, which showed that the chickens had died of bird flu. None of the chickens were vaccinated. Vietnam currently has three provinces with this disease, two in the south and one in the north.
Source: http://english.vietnamnet.vn/social/2008/05/781086/

20. *May 1, Chicago Tribune* – (National) **Health officials fear return of measles.** Federal health officials warned Thursday that the U.S. could be on the verge of a major outbreak of measles, a viral disease that had been declared wiped out in this country in 2000. The official tally of measles cases between January 1 and April 25 totaled 64, the highest number in six years, officials from the Centers for Disease Control and Prevention said. Although the numbers seem small, two developments could set the stage for a major resurgence in this country: an increase in the numbers of people choosing not to get vaccinated and ongoing outbreaks of the disease in Israel and Europe, CDC officials said.

Source: http://www.chicagotribune.com/features/lifestyle/health/chi-measles_02may02,0,962695.story

21. *May 1, Agence France-Presse* – (International) **China struggles to contain viral epidemic.** Doctors in China are struggling to contain the spread of an intestinal virus that has infected about 3,000 children, killing 21 of them so far, the state press reported Friday. The latest death occurred in the city of Fuyang in Anhui province, the epicenter of the epidemic with 2,946 children infected there as of Friday, according to local health officials. The number of children in Anhui infected with enterovirus 71, or EV71, has risen by nearly 500 since Wednesday, the report said. EV71, which can cause hand, foot, and mouth disease, is highly contagious and spread through direct contact with the mucus, saliva, or feces of an infected person. Young children are most susceptible because of lower immune systems. The disease has spread in Anhui since early March, amid accusations by the Chinese media of a government-led cover-up of the epidemic.
Source: http://afp.google.com/article/ALeqM5h6AwGwtihnaqkFBCsIMKS5EXoFxQ

Government Facilities Sector

22. *May 2, WRAL 5 Raleigh* – (North Carolina) **2 injured in explosion of homemade bomb.** In North Carolina, two men were arrested Wednesday after their homemade bomb exploded prematurely, injuring both, authorities said. An investigation determined that the pair had made several bombs at their home, and one of them tried to throw one out the window of a minivan as they drove past Hobbton Middle and High Schools, authorities said. "It's scary to think that these individuals were going to throw an explosive device out of a vehicle in front of a school," Sampson County's sheriff said in a statement. The State Bureau of Investigation and the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) were called in to assist with the case. ATF agents searched the minivan and determined no other bombs were inside, authorities said. A pipe bomb was found during a search of the house, and the Cumberland County Sheriff's Office Bomb Squad responded to disarm it. The ATF is investigating the case for possible federal charges.
Source: http://www.wral.com/news/local/story/2820701/

23. *May 1, Sun Herald* – (Mississippi) **Both Harrison County courthouses given all clear.** The Harrison County, Mississippi, courthouses have been given the all-clear and have allowed employees and visitors back in the building after a bomb threat was texted in this morning. Courthouses in Gulfport and Biloxi were evacuated and searched before allowing employees to return.
Source: http://www.sunherald.com/newsupdates/story/530164.html

[Return to top]

Emergency Services Sector

24. *May 2, Bellingham Herald* – (Washington) **Military to join county hazard drill.**

Dozens of military vehicles and aircraft will be in Whatcom County, Washington, on Tuesday while federal, state and local agencies practice disaster response. Officials will pretend a truck containing 4,000 gallons of a toxic chemical en route to the BP Cherry Point Refinery or the Alcoa Intalco Works aluminum plant exploded, injuring or killing hundreds. Much of the drill will occur near Camp Horizon, in the Birch Bay area. The staged event will begin with North Whatcom Fire and Rescue and Whatcom County Sheriff's Office units arriving on scene, where local high school students will be posing as victims. Washington National Guard, the Federal Emergency Management Agency, and U.S. Army officials will respond as firefighters realize the extent of the injuries.
Source: http://www.bellinghamherald.com/102/story/397971.html

25. *May 1, Washington Post* – (District of Columbia) **D.C. forging surveillance network.** The District of Columbia government is launching a system today that would tie together thousands of city-owned video cameras, but authorities do not yet have the money to complete the high-tech network or privacy rules in place to guide it. The system will feature round-the-clock monitoring of the closed-circuit video systems run by nine city agencies. In the first phase, about 4,500 cameras trained on schools, public housing, traffic, and government buildings will feed into a central office at the D.C. Homeland Security and Emergency Management Agency. Hundreds more will be added this year. By making all those images available under one roof, officials hope to increase efficiency and improve public safety and emergency response. But civil libertarians and D.C. Council members say the network is being rushed into place without sufficient safeguards to protect privacy.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/04/30/AR2008043003430.html?hpid=topnews

[Return to top]

Information Technology

26. *May 2, Computerworld* – (National) **Forrester: IT must prove need for disaster recovery tools.** A Forrester Research Inc. survey of 250 disaster recovery professionals last October found that during the five year period, 27 percent of companies were forced to declare at least one disaster, which the researcher defines as an event that requires activation of a disaster recovery plan. "IT knows their [systems] are vulnerable and it keeps them up at night," an analyst said. "They want to do something about it but it's very hard to get funding for disaster recovery because you can't necessarily use models like return on investment (ROI) and total cost of ownership (TCO)." She suggested that companies consider disaster recovery investment as a rolling upgrade that consistently augments existing infrastructure and application investments rather than a one-time event that can be delayed.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9081979&taxonomyId=17&intsrc=kc_top

27. *May 2, Techworld* – (National) **Botnet attacks military systems.** Security researchers at BitDefender have discovered a complex spamming scheme that hijacks users' PCs in

order to attempt to send junk mail via university and military systems. Researchers said the scheme, based on a backdoor called Edunet, was one of the most complicated and mysterious they have come across. The scam starts with junk emails that offer links to videos. When a user clicks on the link he is prompted to download a "media player." The "media player" download is in fact the Edunet backdoor, which creates a botnet used to attempt to send spam via a list of mail servers, BitDefender said. One of the curiosities of Edunet is that these mail servers are mostly in the .edu and .mil domains. On these servers the botnet looks for open relays - a type of misconfiguration often used by spammers to disguise the real origins of the junk mail. So far, the scheme does not seem to have been very effective, since none of the targeted servers actually host open relays, BitDefender said.
Source:
http://www.pcworld.com/businesscenter/article/145416/botnet_attacks_military_systems.html

28. *May 1, Computerworld* – (International) **Nigerian gets 18 months for cyberattack on NASA employee.** A Nigerian man has been sentenced to 18 months in prison for wooing a NASA employee so he could sneak malware onto her work computer and steal passwords, banking information, and 25,000 screenshots. The man pleaded guilty and was sentenced to 18 months in prison by the Lagos State High Court in Nigeria late last month. He was initially charged with four counts but pleaded guilty to two counts of obtaining goods by false pretenses and forgery. The U.S. attorney for the District of Columbia said the man did not target the woman because she worked for the government. He tried to scam several hundred women and was successful with several. The man, posing as a Texan by using a phony picture and background information, courted the woman for several weeks before he sent an e-mail to her work address with an attachment that contained a phony photo of his phony persona. When she opened the attachment to see the picture, her system was automatically infected with a commercially available piece of spyware. The spyware, which did not spread to other computers on the NASA network, was first downloaded onto her computer on November 21, 2006. It harvested private e-mail, the woman's passwords, her Social Security number, driver's license information, and her home address before it was detected on December 7. During those few weeks, it also captured 25,000 screenshots of whatever she had on her screen at the time, according to a U.S. Department of Justice official, who worked on the investigation, but asked not to be identified.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9081838&taxonomyId=17&intsrc=kc_top

29. *May 1, MessageLabs* – (International) **Web-based malware escalates while Storm calms down.** Analysis performed by MessageLabs shows that during April, the Storm botnet has dramatically decreased to just five percent of its original size, while web-based malware has increased by 23.3 percent. The introduction of new malicious software removal tools, which are aimed at targeting and removing Storm infections, are deemed responsible for the sudden reduction in Storm-infected machines, now estimated at approximately 100,000 compromised computers. Previously estimated at two million,

the decline in Storm's botnet size is evident by the 57 per cent decrease in malware-laden emails distributed by the Storm botnet during April. At the same time, analysis of web-based malware identified that 36.1 percent of interceptions in April were new, an increase of 23.3 percent since March. MessageLabs also identified an average of 1,214 new websites per day harboring malware and other potentially unwanted programs such as spyware and adware, an increase of 619 per day compared with the previous month.
Source: http://www.marketwire.com/mw/release.do?id=850767

30. *May 1, Engadget* – (National) **Researchers design "malicious circuits," warn of potential risk.** A group of researchers from University of Illinois at Urbana-Champaign are now warning that we may see a dramatic increase in hardware-delivered computer viruses. They have apparently managed to develop their own "malicious circuits," which they say can interfere with a computer at a deeper level than a virus, completely bypassing traditional anti-virus software. To accomplish that slightly unsettling feat, the researchers created a replica of the open source Leon3 processor, and added about 1,000 malicious circuits not present in the original processor. Once they hooked that up to another computer they were apparently not only able to swipe passwords from memory, but install malware that would allow the operating system to be remotely controlled as well. Of course, they admit that sneaking such malicious circuits onto a chip is not easy, given that someone would either need to have access to a chip during its manufacturing process, or have the ability to manufacture their own.
Source: http://www.engadget.com/2008/05/01/researchers-design-malicious-circuits-warn-of-potential-risk/

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: http://www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

Nothing to Report

[Return to top]

Commercial Facilities Sector

Nothing to Report

[Return to top]

National Monuments & Icons Sector

Nothing to Report

[Return to top]

Dams Sector

31. *May 2, Associated Press* – (Pennsylvania) **Audit: Pa. needs to improve dam safety enforcement.** Pennsylvania's environmental agency has failed to ensure that all of the state's dams undergo required inspections and is lax on penalizing dam owners for violations, a state audit found. Those findings and other concerns show that the Department of Environmental Protection (DEP) needs to do a better job of managing its dam safety program, the auditor general said Thursday. The DEP's top official responded by saying the agency has already addressed most of the concerns raised in the audit under an effort begun by Pennsylvania's governor more than four years ago. The audit examined records from July 1, 2002, to September 18, 2006. It found that 75 percent of the state's high hazard dams were operating without adequate emergency plans detailing how residents will be informed and evacuated if a dam breaks or overflows.
Source: http://ydr.inyork.com/ci_9119467

32. *May 1, Broken Arrow Ledger* – (Oklahoma) **Tulsa levee gets 'unacceptable' rating.** The U.S. Army Corps of Engineers, Tulsa District, today released an Inspection Report of the Tulsa/West Tulsa Levee with an unacceptable rating. The unacceptable rating means the levee is not currently eligible for federal rehabilitation assistance should the levee be damaged during a flood event. The deficiencies in the inspection report have been noted on previous inspections while the levee continued to be rated "acceptable." The Corps inspection program was standardized following Hurricane Katrina, and all Corps-inspected levees in the nation are being held to high standards to ensure they protect the people and places dependent upon them. Although many aspects of the levee system are well maintained, there were two serious deficiencies that caused the unacceptable rating in the report: 1) tree growth on the levee and 2) plugged and damaged drainage relief wells and toe drain manholes.
Source:
http://www.zwire.com/site/news.cfm?newsid=19651860&BRD=2754&PAG=461&dept_id=574063&rfi=6

33. *May 1, Hillsdale Daily News* – (Michigan) **Jonesville monitoring dam's condition.** An emergency order has been issued by the Michigan Department of Environmental Quality (DEQ) stating the Millpond Dam in Jonesville is in imminent danger of failure. The director of the Dam Safety Program inspected the dam on April 18 and determined it to be in hazardous condition. In a letter to the owner of the dam, the DEQ ordered flow to be minimized through the spillway to alleviate pressure on the dam. An evaluation of the spillway must be conducted by June 1 to determine what steps must be taken to repair it. The letter said the hazard potential for the dam was classified as low. Its failure could threaten the river's resources due to the amount of sediment in the Millpond.
Source: http://www.hillsdale.net/news/x514714426

34. *May 1, KBZK 7 Bozeman* – (Montana) **Hyalite dam to get early warning system.** Engineers say that Bozeman's Middle Creek Dam is in good condition, but the question remains, what happens if it bursts? The Gallatin community wants to use $267,000 of homeland security funds to put an early warning system at Hyalite Canyon, and as of late Wednesday afternoon, Montana's governor officially approved those funds, so construction is now set to begin. Should the Hyalite Dam be breached, there would be a 40 foot wall of water and rocks coming out of the canyon, which could put 6,000 lives in danger. "The structural integrity of the dam itself is not an issue" explains a representative of Gallatin County Emergency Management. "The issue is stuff happens. We live in earthquake country, mountains, conditions with heavy snow run off." Source: http://www.montanasnewsstation.com/Global/story.asp?S=8254892&nav=menu227_3

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Removal from Distribution List:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer